IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Tugenberg et al.	)
For:	Secure Memory and Processing System having Laser-Scribed Encryption	)
Serial No.:	09/671,949	)
Filed:	September 27, 2000	)
Examiner:	Nobahar, A.	)
Art Unit:	2132	)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

APPELLANTS' BRIEF

This brief is being filed in furtherance of the NOTICE OF APPEAL, communicated via facsimile on October 24, 2005.

Any fees required under §41.20, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is Motorola, Inc., a Delaware corporation.

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III. STATUS OF CLAIMS

A. Status of all claims in the proceeding

1. Clams rejected: 1-21
2. Claims allowed: none
3. Claims withdrawn from consideration but not canceled: none
4. Claims objected to: none
5. Claims canceled: none

B. Identification of claims being appealed

The claims on appeal are: 1-21

IV. STATUS OF ANY AMENDMENTS AFTER FINAL

No amendments have been filed after final.

V. SUMMARY OF INVENTION

A first aspect of the present invention, which is being appealed, pertains to a secure processing system for a communication device. The secure processing system includes a host processor (16; page 4, lines 33-35), and a secure memory (20) coupled to the host processor (16) by a data bus (18). The secure memory (20; page 5, lines 5-11) includes a laser-scribed encryption key (21), encryption logic circuitry (23) for implementing a symmetric encryption algorithm using the laser-scribed encryption key (21), a plurality of blocking gates (22) coupling the encryption logic circuitry (23) with the laser-scribed encryption key (21), and a memory (24). In connection with the secure processing system, sensitive data is encrypted (page 9, lines 12-15) by the encryption logic circuitry (23) directly using the laser-scribed encryption key (21) and stored (page 9, lines 15-17) as encrypted data in a data storage medium (12). Furthermore, the encrypted data is decrypted (page 10, lines 26-28 and 34-37) by the encryption logic circuitry (23) directly using the laser-scribed encryption key (21) and transferred to the memory (24) for use by the host processor (16; page 11, lines 5-8).

A further aspect of the present invention, which is being appealed, pertains to a secure communication device. The secure communication device includes a host processor (16), a secure memory (20) coupled to the host processor (16) by a data bus (18), the secure memory (20) including a laser-scribed encryption key (21), and a non-secure memory (12) coupled to host processor (16) for storing encrypted data. In connection with the secure communication device, sensitive data is encrypted within the secure memory (20) directly using the laser-scribed encryption key (21) and stored as encrypted data in the non-secure memory (12), and the encrypted data is decrypted within the secure memory (20) directly using the laser-scribed encryption key (21) and stored within the secure memory (24) for use by the host processor (16).

A still further aspect of the present invention, which is being appealed, pertains to a method of using secure information utilizing a secure communication device, the secure communication device comprising a host processor (16), a secure memory (20) coupled to the host processor (16) by a data bus (18), and a non-secure memory (12) coupled to host processor (16) for storing encrypted data, wherein the secure memory (20) includes a laser-scribed encryption key (21) stored therein. The method includes encrypting (206; page 12, lines 29-35) sensitive data within the secure memory directly using the laser-scribed encryption key, and storing (208; page 13, lines 3-7) the encrypted sensitive data in the non-secure memory. The encrypted sensitive data is then decrypted (306; page 14, lines 8-11) within the secure memory directly using the laser-scribed encryption key, and the decrypted sensitive data is stored (308; page 14, lines 11-13) within the secure memory for use by the host processor.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-21 have been improperly rejected under 35 U.S.C. 103(a) as being unpatentable over Janssen et al. (US Patent No. 5,954,817), in view of Cassagnol et al. (US Patent No. 6,385,727).

VII. ARGUMENTS

A. Rejections under 35 U.S.C. 103

The Examiner has rejected claims 1-21 under 35 U.S.C 103(a) as being unpatentable over Janssen et al., '817, in view of Cassagnol, '727. However, in each instance, the rejection has been misapplied, and not properly presented. The specific reasoning outlining the misapplication and improper presentation of the rejection is noted below.

The Federal Circuit has repeatedly emphasized that, with respect to obviousness, the standard for patentability is the statutory standard. The inquiry is whether the claimed subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art. In this regard, see for example, Monarch Knitting Machinery Corp. v. Saulzer Maurat GMBH, 139 F.3d 877, 881, 45 USPQ2d 1977, 1981 (Fed. Cir. 1998).

For purposes of formulating an obviousness type rejection, the Patent and Trademark Office (PTO) has the initial burden of presenting a prima facie case. In re Mayne, 104 F.3d 1339, 1341, 41 USPQ2d 1451 (Fed. Cir. 1997). In order to establish a prima facie case of obviousness, it must be shown that the prior art reference, or references when combined, teach or suggest all of the claim limitations. Pro-Mold and Tool Co. v. Great Lakes Plastics Inc., 75 F.3d 1568, 37 USPQ2d 1626, 1629 (Fed. Cir. 1996), In re Royka, 490 F.2d 981, 180 USPQ 580, 583 (CCPA 1974). Furthermore, the showing of a suggestion, teaching, or motivation to combine prior teachings "must be clear and particular." In re Dembiczak, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999). These requirements are consistent with the Patent and Trademark Office's own examination guidelines governing the formation of obvious type rejections, see MPEP §2142.

1. Whether claims 1-21 have been improperly rejected under 35 U.S.C. 103(a) as being unpatentable over Janssen et al. (US Patent No. 5,954,817), in view of Cassagnol et al. (US Patent No. 6,385,727).

In attempting to reject claims, the Examiner notes that minimally Janssen et al., '817, fails to teach or suggest sensitive data being encrypted by encryption logic circuitry directly using the laser-scribed encryption key and stored as encrypted data in a data storage medium, and the encrypted data is decrypted by the encryption logic circuitry directly using the laser-scribed encryption key and transferred to the memory for use by the host processor. In fact Janssen et al., '817, is silent and could be said to teach away from the encryption or decryption of the data to be stored or retrieved from an external memory, where more specifically, at least an ESN 205 and the MAC 207 stored in the EEPROM 204 are expressly identified as not being encrypted (col. 5, lines 59-60; see also col. 7, lines 10-15). Janssen et al., '817, is alternatively concerned with the detection of the authenticity of the data and the detection as to whether the programming has been modified through an unauthorized procedure. As a result, it is far from clear whether such a combination of references is even possible, where Janssen et al., '817, relates to instances where the externally stored data is expressly unencrypted, where at least some of the data is then used to communicate with the network.

However, even if one were to attempt to combine the references as suggested by the Examiner, absent any teaching to do so from the references themselves, contrary to the Examiner's assertions, the teachings of Cassagnol et al., '727, would still fails to account for the above noted deficiencies, in so far as Cassagnol et al., '727, similarly minimally fails to make known or obvious the same, in a manner which would make known or obvious the claims of the present application. Cassagnol et al., '727, alternatively describes the use of a combination of keys including a session key, as well as a master key and a device key, for use in encrypting and decrypting the data, at least some of which can not be said to be equivalent to and/or obvious modification of a laser-scribed encryption key associated with the secure processing system as provided for by the claims of the present application, such that the same could be said to make known or obvious the direct encryption and decryption using the laser inscribed key. Alternatively, Cassagnol et al., '727, appears to involve a session key (col. 20, lines 52-55), which is specific to the particular current transaction, and further involves a master key (col. 20, lines 65-67), which appears to be related to a particular software import/export, as well as a device key (col. 11, lines 40-64). Cassagnol et al., '727, still further discusses key cycling on a whitening key (col. 9, lines 48-57 and col. 16, lines 49-52), so as to expressly insure that the same data stored at different times will have different values.

In response to Applicants' remarks in the response to the first Office Action, the Examiner generally notes language in each of Cassagnol et al., '727, (col. 7, line 63 to col. 8, line 20), and Jenssen et al., '817, (col. 5, lines 49-54), which generally suggests other encryption techniques could be used. However, this is not the same as providing a specific teaching, which could reasonably be said to make up for a lack of a specific teaching from the cited references relative to a specific feature in the present claims. Open ended language about further possibilities, does not give the Examiner the freedom to read in a specific teaching that has not been shown to be taught or suggested in the prior art, which presently includes the references being relied upon by the Examiner in support of the rejection.

Consequently, not only would one skilled in the art not be motivated to combine the teachings as suggested by the Examiner, but even if they were to attempt to combine the references as suggested by the Examiner, the references still would not teach or suggest each and every feature of the claims. As a result, the present rejection can hardly be said to have properly shown that the claims would be known or obvious in view of the references being cited. The above noted distinctions are directly applicable to independent claims 1, 12 and 19. Furthermore to the extent that dependent claims 2-11, 13-18 and 20-21, would serve to provide for still further features, the still further features would only serve to further distinguish the claims from the references being cited, where the distinctions relative to the independent claims similarly apply to each of the claims, which depends therefrom.

In view of the above analysis, the applicants would assert, that the Examiner has failed to establish that any of the cited references either separately or in combination make known or obvious each and every feature of any of the presently pending claims, or that one skilled in the art would be motivated to combine the references as suggested. The applicants would respectfully request that the Examiner's decision to finally reject the presently pending claims be overturned, and that the claims be permitted to proceed to allowance.

Respectfully submitted,

BY:

Lawrence J. Chapa
Reg. No. 39,135
Phone No.: (847) 523-0340

Motorola, Inc.
Mobile Devices
Intellectual Property Department
600 North US Highway 45, AS437
Libertyville, IL 60048

VIII. CLAIMS APPENDIX

The following is the text of the claims involved in this appeal:

1. A secure processing system for a communication device comprising:

a host processor; and

a secure memory coupled to the host processor by a data bus, wherein the secure memory comprises:

a laser-scribed encryption key;

encryption logic circuitry for implementing a symmetric encryption algorithm using the laser-scribed encryption key;

a plurality of blocking gates coupling the encryption logic circuitry with the laser-scribed encryption key; and

a memory,

wherein sensitive data is encrypted by the encryption logic circuitry directly using the laser-scribed encryption key and stored as encrypted data in a data storage medium, and

wherein the encrypted data is decrypted by the encryption logic circuitry directly using the laser-scribed encryption key and transferred to the memory for use by the host processor.

2. The processing system as claimed in claim 1 wherein the memory is a zeroizable memory having a zeroizing input that causes the contents of the memory to be erased when a zeroize signal is received on the zeroizing input, and

wherein said zeroize signal is sent to the zeroizable memory by a system monitor upon the occurrence of one of a plurality of predetermined conditions.

3. The processing system as claimed in claim 1 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a non-volatile memory.

4. The processing system as claimed in claim 3 wherein the non-volatile memory includes a portion internal to the integrated circuit chip and a portion external to the integrated circuit chip, and wherein the encrypted data is stored on the portion internal to the integrated circuit chip when the portion internal is available.

5. The processing system as claimed in claim 1 wherein the blocking gates are comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry.

6. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is stored in a one-time programmable memory element.

7. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is stored in non-volatile memory selected from one of the group consisting of ROM, EEPROM, MRAM (Magnetoresistive RAM), battery backed RAM or DRAM and fast logic.

8. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems.

9. The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by burning one-time programmable fuses on a semiconductor die to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems.

10. The processing system as claimed in claim 1 wherein the symmetric encryption algorithm is a block cipher encryption algorithm.

11. The processing system as claimed in claim 1 wherein the host processor is coupled to an external memory having a secret key stored therein in encrypted form, the secret key being encrypted with the laser-scribed encryption key, and said secret key being used for secure communication between the communication device and other communication devices.

12. A secure communication device comprising:

a host processor;

a secure memory coupled to the host processor by a data bus, the secure memory including a laser-scribed encryption key; and

a non-secure memory coupled to host processor for storing encrypted data,

wherein sensitive data is encrypted within the secure memory directly using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, and

wherein the encrypted data is decrypted within the secure memory directly using the laser-scribed encryption key and stored within the secure memory for use by the host processor.

13. The communication device as claimed in claim 12 wherein the non-secure memory has a secret key stored therein in encrypted form, the secret key being encrypted with the laser-scribed encryption key, and said secret key being used for secure communication between the communication device and other communication devices.

14. The communication device as claimed in claim 12 wherein the communication device is a data communication device, and wherein the secret key is a private key unique to a user of the communication device and is part of a public-private key pair, the private key being used for decrypting data sent to said user, and wherein prior to using said secret key, said secret key being decrypted by encryption logic of the secure memory using the laser-scribed encryption key and stored in unencrypted form in a zeroizable memory.

15. The communication device as claimed in claim 14 wherein the data communication device is adapted for transmitting data to another communication device, and wherein the secret key is further used to generate a digital signature associated with said data, said digital signature being transmitted along with said data.

16. The communication device as claimed in claim 12 wherein the communication device is a wireless communication device for communicating secured voice, and wherein the secret key is used for generating a common session key for communicating with another communication device,

and wherein prior to using said secret key, said secret key being decrypted by encryption logic of the secure memory using the laser-scribed encryption key and stored in unencrypted form in zeroizable memory.

17. The communication device as claimed in claim 12 wherein the secret key is one of a plurality of secret encryption keys stored in encrypted form in the non-secure memory, the plurality of secret keys being encrypted with the laser-scribed encryption key, and

wherein one of the secret keys of the plurality is selected for secure communication between the communication device and other communication device, and wherein a zeroizable memory is cleared after communication with the other communication device, and

wherein prior to using said selected secret key, said selected secret key is decrypted by the encryption logic using the laser-scribed encryption key and stored in unencrypted form in the zeroizable memory.

18. The communication device as claimed in claim 12 wherein the secure memory further comprises:

a plurality of blocking gates coupled to the laser-scribed encryption key;

encryption logic circuitry for implementing a symmetric encryption algorithm using the laser-scribed encryption key and coupled to the blocking gates; and

a zeroizable memory coupled to the encryption logic circuitry,

wherein sensitive data is encrypted by the encryption logic circuitry using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, and

wherein the encrypted data is decrypted by the encryption logic circuitry with the laser-scribed encryption key and transferred to the zeroizable memory for use by the host processor.

19. A method of using secure information utilizing a secure communication device, the secure communication device comprising a host processor, a secure memory coupled to the host processor by a data bus, and a non-secure memory coupled to host processor for storing encrypted data, wherein the secure memory includes a laser-scribed encryption key stored therein, the method comprising the steps of:

encrypting sensitive data within the secure memory directly using the laser-scribed encryption key;

storing the encrypted sensitive data in the non-secure memory;

decrypting the encrypted sensitive data within the secure memory directly using the laser-scribed encryption key; and storing the decrypted sensitive data within the secure memory for use by the host processor.

20. The method as claimed in claim 19 wherein the secure memory includes blocking gates coupled between encryption logic circuitry and the laser-scribed encryption key, and a zeroizable memory coupled to the encryption logic circuitry, and wherein the storing step comprises storing the decrypted sensitive data within the zeroizable memory, and wherein the method further comprises the steps of:

disabling the blocking gates during the encrypting and decrypting steps; and

zeroizing the zeroizable memory after the host processor is through using the decrypted sensitive data stored in the zeroizable memory.

21. The method as claimed in claim 20 further comprising the step of enabling the blocking gates preventing the encryption logic circuitry from accessing the laser scribed encryption key, the step of enabling being performed upon completion of the decrypting step.